(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年7 月21 日 (21.07.2005)

PCT

(10) 国際公開番号
WO 2005/067200 A1

(51) 国際特許分類[7]: H04L 9/32, 9/14

(21) 国際出願番号: PCT/JP2004/005879

(22) 国際出願日: 2004 年4 月23 日 (23.04.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2003-432447
2003 年12 月26 日 (26.12.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 大越 丈弘 (OHKOSHI, Takehiro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 山田 敬喜 (YAMADA, Keiki) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 牧田 覚 (MAKITA, Satoru) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP).

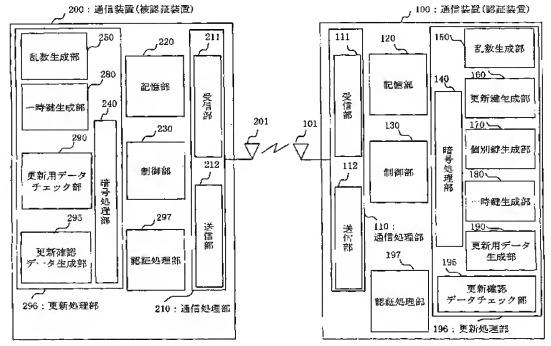
(74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

/続葉有/

(54) Title: AUTHENTICATION DEVICE, DEVICE TO BE AUTHENTICATED, AND KEY UPDATE METHOD

(54) 発明の名称: 認証装置及び被認証装置及び鍵更新方法



200...COMMUNICATION DEVICE (DEVICE TO BE AUTHENTICATED)
250...RANDOM NUMBER GENERATION SECTION
280...TEMPORARY KEY GENERATION SECTION
290...UPDATE DATA CHECK SECTION
295...UPDATE CONFIRMATION DATA GENERATION SECTION
240...ENCRYPTION PROCESSING SECTION
296...UPDATE PROCESSING SECTION
220...STORAGE SECTION
230...CONTROL SECTION
297...AUTHENTICATION PROCESSING SECTION
211...RECEPTION SECTION
212...TRANSMISSION SECTION
210...COMMUNICATION PROCESSING SECTION
100...COMMUNICATION DEVICE (AUTHENTICATION DEVICE)
111...RECEPTION SECTION
112...TRANSMISSION SECTION
120...STORAGE SECTION
130...CONTROL SECTION
110...COMMUNICATION PROCESSING SECTION
197...AUTHENTICATION PROCESSING SECTION
140...ENCRYPTION PROCESSING SECTION
150...RANDOM NUMBER GENERATION SECTION
160...UPDATE KEY GENERATION SECTION
170...INDIVIDUAL KEY GENERATION SECTION
180...TEMPORARY KEY GENERATION SECTION
190...UPDATE DATA GENERATION SECTION
195...UPDATE CONFIRMATION DATA CHECK SECTION
196...UPDATE PROCESSING SECTION

(57) Abstract: An authentication device (100) includes: an authentication processing section (197) for performing authentication of a communication device (200) by using an authentication key; and an update key generation key section (160)for generating a new authentication key when the communication device (200) does not have an authentication key to be used for the authentication processing by the authentication processing section (197) and generating a new authentication key for updating the authentication key when the communication device (200) has an authentication key but authentication of the communication device (200) by the authentication processing section (197) has failed. By using the new authentication key generated by the update key generation section (160), the authentication processing section (197) again performs authentication of the communication device (200).

(57) 要約: 認証装置１００に、認証用鍵を用いて通信装置２００との間で認証処理をおこなう認証処理部１９７と、上記認証処理部１９７による認証処理に用いる認証用鍵を通信装置２００が保持していない場合に新たな認証用鍵を生成し、上記通信装置２００が保持している場合で上記認証処理部１９７による通信装置２００との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部１６０とを備え、上記認証処理部１９７は、上記更新鍵生成部１６０によ

/続葉有/

WO 2005/067200 A1

BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

り生成された新たな認証用鍵を用いて通信装置２００との間での認証処理を再度おこなうことを特徴とする。

明細書

認証装置及び被認証装置及び鍵更新方法

技術分野

本発明は、認証装置、被認証装置、或いは両者の鍵更新方法に関する。特に、ＥＴＣ（ノンストップ自動料金支払いシステム）やドライブスルー等、無線通信機能を有する移動体及び移動体通信システムに関する。

背景技術

利用者があるサービスを受けるとき、サービスを受けられる正当な利用者であるか本人確認（認証）が行われる。その際、鍵なし・期限切れ等の理由により認証に失敗するとサービスを受けることができない。

利用者は、鍵の更新等正当な利用者であるための手続きを怠ると、たとえ正当な利用者であっても（不正を行う意図はなくとも)、サービスを受けることができなくなるといった問題があった。

また、特開２００３－１９６２４０号公報に記載の技術では、テンポラリで認証が許可されてしまうため、過去に認証に成功していれば、その後何度でも認証されてしまい、認証装置にアクセス可能となることからセキュリティホールになりかねないといった問題があった。

また、特開平１１－２７４９９９号公報，特開２０００－１３８６７４号公報，特開２０００－１９６５８８号公報に記載の技術では、双方が保持している鍵の中から、使用鍵を決定しているに過ぎず、鍵更新をおこなうことができないといった問題があった。

本発明は、鍵更新をおこなうことで更新された鍵により正当な利用者

に対しては、サービスを提供し、サービスの可用性及び利用者の利便性を向上させることを目的とする。

発明の開示

この発明に係る認証装置は、認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、

上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持していない場合に新たな認証用鍵を生成し、上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持している場合で上記認証処理部による上記被認証装置との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部とを備え、

上記認証処理部は、上記更新鍵生成部により生成された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする。

また、上記認証装置は、さらに、

被認証装置から所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部を備え、

上記更新鍵生成部は、上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記新たな認証用鍵を生成し、

上記認証装置は、さらに、

上記更新鍵生成部により生成された新たな認証用鍵を被認証装置に送信する送信部を備え、

上記認証処理部は、上記送信部により送信された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とす

る。

この発明に係る被認証装置は、所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する記憶部と、

認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、

上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいた新たな認証用鍵を受信する受信部と

を備え、

上記認証処理部は、上記受信部により受信された新たな認証用鍵を用いて上記認証装置との間での認証処理を再度おこなうことを特徴とする。

また、上記受信部は、上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記認証装置から所定の情報を受信し、

上記送信部は、上記受信部により所定の情報が受信された場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信することを特徴とする。

この発明に係る鍵更新方法は、所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信する第１の送信工程と、

上記第１の送信工程により上記認証装置から送信された所定の情報を上記被認証装置が受信する第１の受信工程と、

上記第１の受信工程により上記所定の情報が受信された後、上記被認証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信する第２の送信工程と、

上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置が受信する第２の受信工程と、

上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子

とに基づいて、上記認証装置が新たな認証用鍵を生成する生成工程と、

上記生成工程により生成された新たな認証用鍵を被認証装置に送信する第３の送信工程と、

上記第３の送信工程により送信された新たな認証用鍵を上記被認証装置が受信する第３の受信工程と、

上記第３の受信工程により受信された新たな認証用鍵を、上記被認証装置と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこなう鍵更新工程と、

更新確認データを生成して上記認証装置へ送信する工程と、

更新確認データを受信し、確認する工程と

を備えたことを特徴とする。

図面の簡単な説明

図１は、実施の形態１における認証システムの構成を示す図である。

図２は、実施の形態１における認証システムの概念を示す図である。

図３は、実施の形態１における鍵更新方法の手順を示すフローチャート図である。

図４は、通信情報１のフレームの一例を示す図である。

図５は、通信情報２のフレームの一例を示す図である。

図６は、通信情報３のフレームの一例を示す図である。

図７は、通信情報４のフレームの一例を示す図である。

図８は、実施の形態２における鍵更新処理に至るまでの手順を示すフローチャート

図である。

図９は、ハードウェア構成図である。

発明を実施するための最良の形態

実施の形態１．

以下に説明するように、被認証装置と認証装置との間での認証時、被認証装置が鍵なし又は被認証装置が有する鍵が有効期限切れであっても、認証失敗とするのではなく、鍵更新手段により鍵更新を実施し、その後、認証を行うものである。

図１は、実施の形態１における認証システムの構成を示す図である。

図１において、認証システムは、認証装置となる通信装置１００と被認証装置となる通信装置２００とを備えている。通信装置１００は、アンテナ１０１、通信処理部１１０、記憶部１２０、制御部１３０、更新処理部１９６、認証処理部１９７を備えている。通信処理部１１０は、受信部１１１、送信部１１２を有している。更新処理部１９６は、暗号処理部１４０、乱数生成部１５０、更新鍵生成部１６０、個別鍵生成部１７０、一時鍵生成部１８０、更新用データ生成部１９０、更新確認データチェック部１９５を有している。通信装置２００は、アンテナ２０１、通信処理部２１０、記憶部２２０、制御部２３０、更新処理部２９６、認証処理部２９７を備えている。通信処理部２１０は、受信部２１１、送信部２１２を有している。更新処理部２９６は、暗号処理部２４０、乱数生成部２５０、一時鍵生成部２８０、更新用データチェック部

２９０、更新確認データ生成部２９５を有している。実施の形態１では、通信装置１００と通信装置２００とは、アンテナ１０１，２０１を介して無線通信する場合を説明するが、これに限るものではなく有線通信であっても構わない。例えば、ＥＴＣ（料金自動収集）、ドライブスルー等において、通信装置１００は、店舗側の路側機として、通信装置２００は、自動車側の車載機として構成される。

図２は、実施の形態１における認証システムの概念を示す図である。

例えば、ＥＴＣ、ドライブスルー等において、通信装置１００は、店舗側の路側機として、通信装置２００は、自動車側の車載機として構成される場合、ＥＴＣ、ドライブスルー等によるサービス提供において、店舗側の路側機は、起動後、認証処理を実施する状態で、利用者（自動車）の来店（通過）を待ち続ける。

利用者が来店すると、路側機は自動車に設置された車載機に対して認証要求を送信する。

車載機は路側機の指示にしたがって必要な情報を路側機に送信する。

路側機は、車載機から受け取った情報が古い或いは鍵がないと判断した場合、鍵更新の状態となり、車載機に対して鍵更新要求を実施する。

車載機は、路側機の指示にしたがって鍵更新を実施する。

鍵更新終了後、路側機は認証状態となり、車載機に対して認証処理を実施する。

言い換えれば、本実施の形態１における認証システム或いは認証方式は、鍵更新手段を備えている。そして、認証処理と更新処理が分離している。認証処理中は、更新処理はされない。

そして、鍵情報が古い又はない場合、鍵更新を実施してから認証処理を実施する。すなわち、初期時（鍵情報がないとき）、鍵更新処理を実施する。或いは、通常運用時は認証処理を実施して、認証に用いる鍵情

報が古い場合、鍵更新処理を実施する。

図３は、実施の形態１における鍵更新方法の手順を示すフローチャート図である。

記憶部１２０は、所定のアルゴリズム識別子と所定の暗号鍵識別子と、上記所定のアルゴリズム識別子に対応するアルゴリズムを記憶している。

記憶部２２０は、所定のアルゴリズム識別子と所定の暗号鍵識別子と、上記所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵と装置固有番号とを記憶している。また、上記記憶部２２０は、古くなった或いは使用期限が過ぎた認証用鍵及びその認証用鍵の識別子を記憶している。或いは、記憶部２２０は、認証用鍵を記憶していない場合であってもよい。ここで、所定の暗号鍵識別子は、鍵更新専用の鍵の識別子（更新用識別子）である。所定の暗号鍵識別子に対応する暗号鍵は、鍵更新専用鍵である。この鍵更新専用の鍵の識別子及び鍵更新専用鍵は、初期時（例えば装置の出荷時）における新規鍵生成に伴う鍵更新処理、或いは通常運用時に発生した鍵更新処理において、通信装置１００，２００間で互いに共有できる認証用鍵が存在しない緊急時における別の新たな鍵生成に伴う鍵更新処理のいずれかの場合に用いる。認証処理に用いることはない。

まず、認証処理部１９７は、被認証装置となる通信装置２００との間で認証処理をおこなう。言い換えれば、認証処理部２９７は、認証装置となる通信装置１００との間で認証処理をおこなう。認証処理の際、認証用鍵を用いておこなう。ここで、記憶部２２０が、古くなった或いは使用期限が過ぎた認証用鍵を記憶している場合、或いは、記憶部２２０が、認証用鍵を記憶していない場合、認証用鍵が使用できないので、ここでの認証処理は失敗に終わることになる。

Ｓ（ステップ）２０１において、乱数生成工程として、上記認証処理が失敗に終わると、乱数生成部１５０は、乱数１を生成する。

Ｓ２０２において、送信工程として、送信部１１２は、乱数生成部１５０により生成された乱数１（所定の情報の一例である）を通信情報１として通信装置２００に送信する。通信装置１００は、乱数１を通信情報１として通信装置２００に送信することで、認証処理から鍵更新処理に移行したことを通信装置２００へ知らせることになる。

Ｓ２０３において、受信工程として、受信部２１１は、送信部１１２により送信された乱数１を通信情報１として受信する。通信装置２００では、受信部２１１が、乱数１を受信したことにより、通信装置１００より鍵更新が要求されたと判断する。

Ｓ２０４において、認証処理工程の一部として、乱数生成部２５０は、乱数２を生成する。

Ｓ２０５において、送信工程として、送信部２１２は、上記記憶部２２０により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子と装置固有番号と、乱数生成部２５０により生成された乱数２とを通信情報２として認証装置である通信装置２００に送信する。存在する場合には、古くなった或いは使用期限が過ぎた認証用鍵の識別子と対応するアルゴリズムの識別子とを一緒に送信する。ここで、１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組みとしてプロファイルとして表し、通信情報２は、乱数２と装置固有番号と組数分のプロファイル数とプロファイル数分の各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とをデータとして有している。さらに、ここでは、各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とを対応させたデータとしている。言い換えれば、上

記送信部２１２は、上記記憶部２２０により１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組のプロファイルとして記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置となる通信装置１００に送信する。

Ｓ２０６において、受信工程として、受信部１１１は、被認証装置となる通信装置２００から、乱数２と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも１つのプロファイル識別子と少なくとも１つのプロファイル識別子の各プロファイル識別子に対応した少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを有する通信情報２を受信する。

Ｓ２０７において、生成工程として、更新鍵生成部１６０は、上記受信部１１１により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記鍵更新専用の鍵の識別子である所定の暗号鍵識別子と所定の暗号鍵識別子に対応する上記所定のアルゴリズム識別子とを選択する。そして、更新鍵生成部１６０は、上記受信部１１１により受信された装置固有番号等とたとえばハッシュ値等を用いて更新鍵となる新たな認証用鍵を生成する。言い換えれば、更新鍵生成部１６０は、上記受信部１１１により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記認証処理部１９７による認証処理に用いる認証用鍵を上記被認証装置となる通信装置２００が保持していない場合に新たな認証用鍵を生成し、上記認証処理部１９７による認証処理に用いる認証用鍵を上記被認証装置となる通信装置２００が保持している場合で上記認証処理部１９７による上記被認証装置となる通信装置２００との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する。

Ｓ２０８において、個別鍵生成工程として、個別鍵生成部１７０は、

上記更新鍵生成部１６０により選択された所定の暗号鍵識別子に対応する暗号鍵となる通信装置２００が有している鍵更新専用鍵となる個別鍵を更新鍵生成部１６０と同様の方法で生成する。

Ｓ２０９において、一時鍵生成工程として、一時鍵生成部１８０は、上記更新鍵生成部１６０により選択された所定のアルゴリズム識別子に対応するアルゴリズムを用いて所定の暗号鍵識別子に対応する暗号鍵となる個別鍵生成部１７０により生成された個別鍵で乱数１，２を暗号処理部１４０を用いて暗号化し、鍵更新処理用暗号鍵の一例となる一時鍵を生成する。

Ｓ２１０において、更新用データ生成工程として、更新用データ生成部１９０は、乱数２のすべて或いは一部と、更新鍵となる新たな認証用鍵とを暗号処理部１４０により一時鍵生成部１８０により生成された一時鍵で暗号化することにより更新用データを生成する。

Ｓ２１１において、送信工程として、送信部１１２は、上記更新鍵生成部１６０により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のプロファイル識別子と更新用データ生成部１９０により生成された更新用データとを通信情報３として上記被認証装置となる通信装置２００に送信する。

Ｓ２１２において、受信工程として、受信部２１１は、上記認証装置となる通信装置１００から上記送信部２１２により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のアルゴリズム識別子と所定の暗号鍵識別子とに対応するプロファイル識別子と更新用データとを通信情報３として受信する。言い換えれば、上記受信部２１１は、上記認証装置となる通信装置１００から上記送信部２１２により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいた新たな認証用鍵を受信する。

Ｓ２１３において、確認工程として、暗号処理部２４０は、受信部２１１により受信されたプロファイル識別子を確認し、プロファイル識別子に対応する所定の暗号鍵識別子と所定のアルゴリズム識別子とを確認する。

Ｓ２１４において、一時鍵生成工程として、一時鍵生成部２８０は、受信部２１１により受信され、暗号処理部２４０により確認された所定のアルゴリズム識別子に対応するアルゴリズムを用いて、記憶部２２０に記憶された個別鍵で乱数１，２を暗号処理部２４０を用いて暗号化し、更新処理用暗号鍵の一例となる上記一時鍵を生成する。以上により通信装置１００，２００間で同じ一時鍵という鍵共有ができたことになる。なお、この実施形態では、一時鍵生成部１８０，２８０が一時鍵生成の際、個別鍵で暗号化したが、認証装置と被認証装置とが同じ処理を実施すればよいため、復号してもよい。

Ｓ２１５において、更新用データチェック工程として、更新用データチェック部２９０は、受信部２１１により通信情報３として受信された暗号化されている更新用データを一時鍵生成部２８０により生成された一時鍵により暗号処理部２４０を用いて復号する。

Ｓ２１６において、鍵更新工程の一部として、更新用データチェック部２９０は、復号した更新用データのデータが、通信装置２００が通信装置１００に送信した乱数２のすべて或いは一部であるかどうかを確認する。復号した更新用データのデータが乱数２のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置１００との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置１００，２００間での認証処理の一方が成功したことを意味する。そして、更新用データチェック部２９０は、復号することによって得られた上記受信部２１１により受信された新たな認証用鍵を、上記

通信装置１００と通信装置２００との間での認証処理をおこなうための更新鍵として鍵更新をおこなう。更新鍵は、記憶部２２０に記憶される。

Ｓ２１７において、更新確認データ生成工程として、更新確認データ生成部２９５は、乱数１のすべて或いは一部を暗号処理部２４０により一時鍵生成部２８０により生成された一時鍵で暗号化することにより更新確認データを生成する。

Ｓ２１８において、送信工程として、送信部２１２は、更新確認データ生成部２９５により生成された更新確認データを通信情報４として通信装置１００に送信する。

Ｓ２１９において、受信工程として、受信部１１１は、通信装置２００から更新確認データを通信情報４として受信する。

Ｓ２２０において、更新確認データチェック工程として、更新確認データチェック部１９５は、受信部１１１により通信情報４として受信された暗号化されている更新確認データを一時鍵生成部１８０により生成された一時鍵により暗号処理部１４０を用いて復号する。

Ｓ２２１において、更新確認データチェック工程として、更新確認データチェック部１９５は、復号した更新確認データのデータが、通信装置１００が通信装置２００に送信した乱数１のすべて或いは一部であるかどうかを確認する。復号した更新確認データのデータが乱数１のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置２００との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置１００，２００間での認証処理の他方が成功したことを意味する。

以上により、通信装置１００，２００間での鍵更新処理が終了し、その後、上記認証処理部１９７は、上記更新鍵生成部１６０により生成さ

れた新たな認証用鍵を用いて上記被認証装置となる通信装置２００との間での認証処理を再度おこなう。言い換えれば、上記認証処理部２９７は、上記受信部２１１により受信された新たな認証用鍵を用いて上記認証装置となる通信装置１００との間での認証処理を再度おこなう。

図４は、通信情報１のフレームの一例を示す図である。

図４において、通信情報１は、ヘッダと乱数１データを有している。

図５は、通信情報２のフレームの一例を示す図である。

図５において、通信情報２は、ヘッダと乱数２データと装置固有番号（装置固有Ｎｏ.）とプロファイル数（Ｐｒｏｆｉｌｅ数）と各プロファイルを識別するプロファイル識別子としてのＰｒｏｆｉｌｅ１，・・・Ｐｒｏｆｉｌｅ　ｎと、各プロファイル識別子に対応するアルゴリズム識別子（アルゴリズムＩＤ）と暗号鍵識別子（鍵ＩＤ）とを有している。プロファイルの最終番号に鍵更新専用の鍵の識別子（更新用識別子）と更新用識別子に対応するアルゴリズム識別子が記載されている。図５では、各プロファイル識別子と各プロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

図６は、通信情報３のフレームの一例を示す図である。

図６において、通信情報３は、ヘッダと選択された所定のプロファイルを識別する所定のプロファイル識別子としてのＰｒｏｆｉｌｅ　ｎと、所定のプロファイル識別子に対応するアルゴリズム識別子（アルゴリズムＩＤ）と暗号鍵識別子（鍵ＩＤ）と更新用データとを有している。図５では、所定のプロファイル識別子と所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

図７は、通信情報４のフレームの一例を示す図である。

図７において、通信情報４は、ヘッダと更新確認データとを有している。

ここで、制御部１３０は、通信装置１００の各部を制御する。また、制御部２３０は、通信装置２００の各部を制御する。また、記憶部１２０は、通信装置１００の各部で行なわれる処理中に生じるデータを記憶する。また、記憶部２２０は、通信装置２００の各部で行なわれる処理中に生じるデータを記憶する。

以上のように、本実施の形態１における鍵更新方法は、所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信する第１の送信工程と、上記第１の送信工程により上記認証装置から送信された所定の情報を上記被認証装置が受信する第１の受信工程と、上記第１の受信工程により上記所定の情報が受信された後、上記被認証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信する第２の送信工程と、上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置が受信する第２の受信工程と、上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記認証装置が新たな認証用鍵を生成する生成工程と、上記生成工程により生成された新たな認証用鍵を被認証装置に送信する第３の送信工程と、上記第３の送信工程により送信された新たな認証用鍵を上記被認証装置が受信する第３の受信工程と、上記第３の受信工程により受信された新たな認証用鍵を、上記被認証装置と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこなう鍵更新工程と、更新確認データを生成して上記認証装置へ送信する工程と、更新確認データを受信し、確認する工程

とを備えている。

また、例えば、ＥＴＣ、ドライブスルー等において、通信装置１００は、店舗側の路側機として、通信装置２００は、自動車側の車載機として構成される場合、以上のように、この認証方式を実施する車載機は、路側機からの指示に従って鍵更新へ状態が切り替わる（鍵更新を実施する）。そして、車載機が自身の判断により鍵更新へ状態が切り替わったり、鍵更新を要求することはない。また、この認証方式を実施する路側機は、車載機に対して鍵情報を要求及びチェックし、必要であれば鍵更新を車載機に指示する。すなわち、路側機主導で処理が行なわれる。

また、ここでは、一例として、ＥＴＣ、ドライブスルー等での自動車（車載機）と路側機（店舗システム）とに適用し、想定したが、通信装置は限定するものではない。例えば、基地局と携帯電話、無線ＬＡＮ（基地局とパソコン）、Ｒ／Ｗ（リーダー／ライター）とＲＦ　Ｔａｇ（電子タグ）といった固定局と移動局とにおける通信はもちろんのこと、モバイルとモバイルの通信等にも適用できる。

以上のように、本実施の形態によれば、鍵なし・期限切れ等の場合であっても鍵の更新をおこなうことができ、その後に正当な利用者がサービスの提供を受けることができ、本発明を利用するシステムのサービスの可用性及び利用者の利便性を向上させることができる。

また、本実施の形態によれば、さらに、セットアップ作業が不要となる。具体的には、例えば、車載機の出荷時及び店舗にて自動車に設置時、暗号通信に用いる鍵等車載機固有情報のセットアップが不要となる。そのため、製造においては同一の車載機を生産することができ生産効率が向上する。車載機固有の情報は、システムのセキュリティを維持するために重要なものであるため、セットアップ時の固有情報の取得は登録・作業者の限定といった細かな制限事項が発生する。しかし、セットア

ップ作業が不要なためどの業者でも設置でき流通コスト及び作業が軽減される。

実施の形態２.

図８は、実施の形態２における鍵更新処理に至るまでの手順を示すフローチャート図である。

Ｓ８０１において、認証処理部１９７は、被認証装置となる通信装置２００との間で認証処理をおこなう。言い換えれば、認証処理部２９７は、認証装置となる通信装置１００との間で認証処理をおこなう。認証処理の際、認証用鍵を用いておこなう。ここで、記憶部２２０が、古くなった或いは使用期限が過ぎた認証用鍵を記憶している場合、或いは、記憶部２２０が、認証用鍵を記憶していない場合、認証用鍵が使用できないので、ここでの認証処理は失敗に終わることになる。

Ｓ８０２において、送信部１１２は、認証処理が失敗に終わったことを示す失敗データを通信装置２００に送信する。

Ｓ８０３において、受信部２１１は、通信装置１００より失敗データを受信する。

Ｓ８０４において、送信部２１２は、失敗データを受信したことを示す確認データ（Ａｃｋ）を通信装置１００に送信（返信）する。

Ｓ８０５において、通信装置１００は、図３に示す鍵更新方法による鍵更新処理を開始する。

実施の形態１では、認証処理部１９７が、認証処理が失敗に終わったと判断した場合に、直ちに図３に示す鍵更新方法による鍵更新処理を開始するが、図８に示すように、認証処理が失敗に終わったことを通信装置１００，２００間で確認した後に鍵更新方法による鍵更新処理を開始するようにしてもよい。

図９は、ハードウェア構成図である。

以上の説明において、各実施の形態の説明において「～部」として説明したものを、一部或いはすべてコンピュータで動作可能なプログラムにより構成する場合、図９に示すように、通信装置１００，２００は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）３７を備えている。ＣＰＵ３７は、内蔵された、或いはバス３８を介してＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）４０（記憶装置、記憶部の一例である）、外部と通信可能な通信ポート４４に接続されている。また、図９に示すように、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）３９、磁気ディスク装置４６等の記憶装置に接続されていても構わない。

プログラムにより構成する場合、図９におけるプログラム群４９には、各実施の形態の説明において「～部」として説明したものにより実行されるプログラムが記憶されている。プログラム群４９は、上記記憶装置に記憶されている。プログラム群４９は、ＣＰＵ３７、ＯＳ４７等により実行される。記憶装置は、各処理の結果を記憶する。

また、各実施の形態の説明において「～部」として説明したものは、ＲＯＭ３９に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

また、上記各実施の形態を実施させるプログラムは、ＦＤ（Ｆｌｅｘｉｂｌｅ Ｄｉｓｋ）、光ディスク、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）等のその他の記録媒体による記録装置を用いて記憶されても構わない。係る場合には、図９に示すように、ＦＤＤ（Ｆｌｅｘｉｂｌｅ Ｄｉｓｋ Ｄｒｉｖｅ）４５、コンパクトディスク装置（ＣＤＤ）８６等を備える。

産業上の利用可能性

このような通信装置１００，２００は、ＥＴＣ、ドライブスルー等における店舗側の路側機と自動車側の車載機に限らず、携帯電話等の移動体通信装置間、有線の通信装置間、或いは基地局を経由した有線と無線の通信装置間等における認証装置、被認証装置として、使用することができる。

本発明によれば、鍵なし・期限切れ等の場合であっても鍵の更新をおこなうことができ、その後に正当な利用者がサービスの提供を受けることができ、本発明を利用するシステムのサービスの可用性及び利用者の便性を向上させることができる。

請求の範囲

1．認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、

上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持していない場合に新たな認証用鍵を生成し、上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持している場合で上記認証処理部による上記被認証装置との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部とを備え、

上記認証処理部は、上記更新鍵生成部により生成された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする認証装置。

2．上記認証装置は、さらに、

被認証装置から所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部を備え、

上記更新鍵生成部は、上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記新たな認証用鍵を生成し、

上記認証装置は、さらに、

上記更新鍵生成部により生成された新たな認証用鍵を被認証装置に送信する送信部を備え、

上記認証処理部は、上記送信部により送信された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする請求項1記載の認証装置。

3．所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する

記憶部と、

認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、

上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいた新たな認証用鍵を受信する受信部と

を備え、

上記認証処理部は、上記受信部により受信された新たな認証用鍵を用いて上記認証装置との間での認証処理を再度おこなうことを特徴とする被認証装置。

4．上記受信部は、上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記認証装置から所定の情報を受信し、

上記送信部は、上記受信部により所定の情報が受信された場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信することを特徴とする請求項3記載の被認証装置。

5．所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信する第1の送信工程と、

上記第1の送信工程により上記認証装置から送信された所定の情報を上記被認証装置が受信する第1の受信工程と、

上記第1の受信工程により上記所定の情報が受信された後、上記被認

証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信する第２の送信工程と、

上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置が受信する第２の受信工程と、

上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子

とに基づいて、上記認証装置が新たな認証用鍵を生成する生成工程と、

上記生成工程により生成された新たな認証用鍵を被認証装置に送信する第３の送信工程と、

上記第３の送信工程により送信された新たな認証用鍵を上記被認証装置が受信する第３の受信工程と、

上記第３の受信工程により受信された新たな認証用鍵を、上記被認証装置と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこなう鍵更新工程と、

更新確認データを生成して上記認証装置へ送信する工程と、

更新確認データを受信し、確認する工程と

を備えたことを特徴とする鍵更新方法。

６．所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信し、

上記認証装置から送信された所定の情報を上記被認証装置が受信し、

上記所定の情報が受信された後、上記被認証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信し、

送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記

認証装置が受信し、

受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記認証装置が新たな認証用鍵を生成し、

生成された新たな認証用鍵を被認証装置に送信し、

送信された新たな認証用鍵を上記被認証装置が受信し、

受信された新たな認証用鍵を、上記被認証装置と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこない、

更新確認データを生成して上記認証装置へ送信し、

更新確認データを受信し、確認することを特徴とする鍵更新方法。

図1

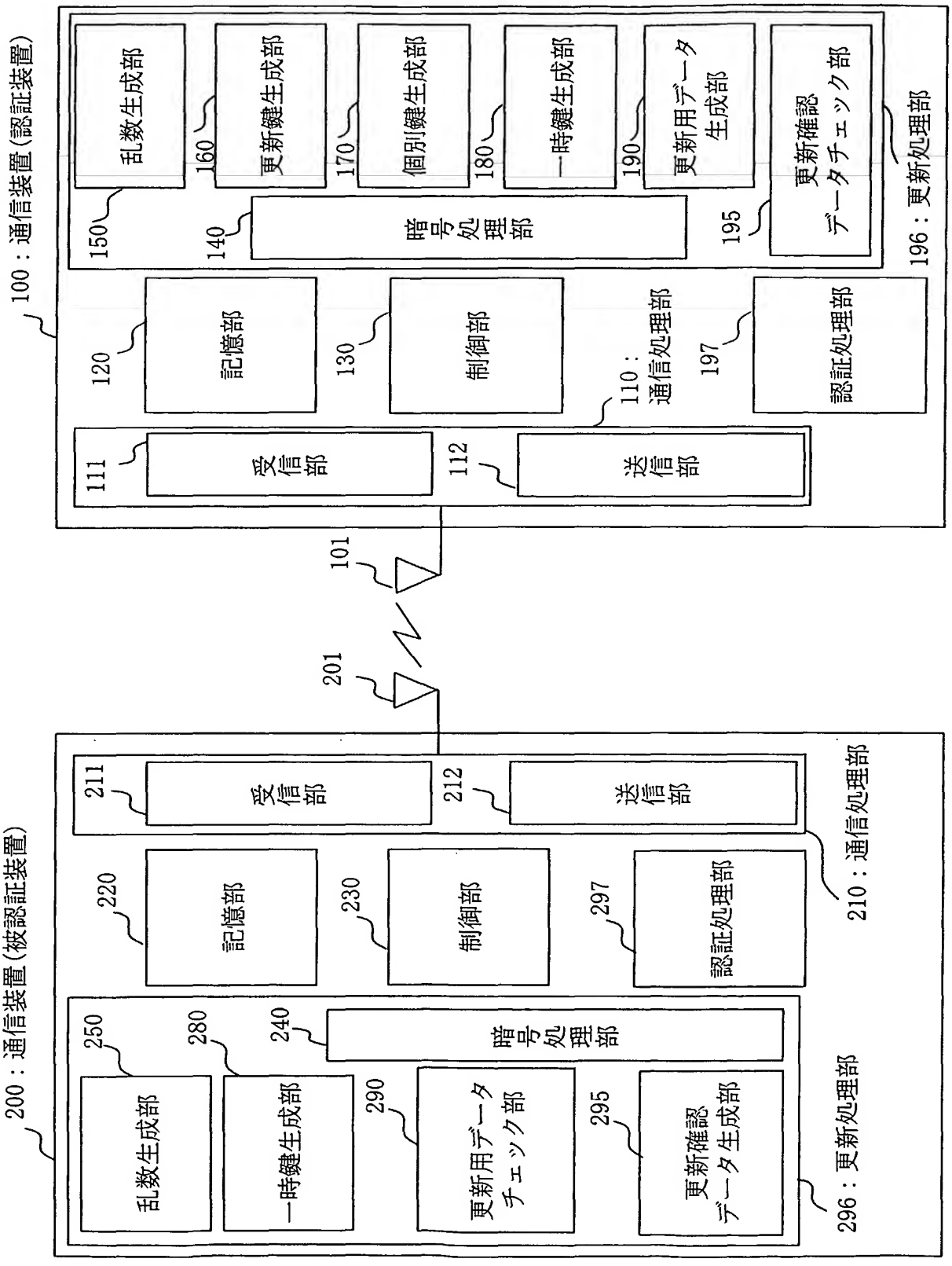

100：通信装置(認証装置)
乱数生成部
150
更新鍵生成部
160
個別鍵生成部
170
一時鍵生成部
180
更新用データ生成部
190
更新確認データチェック部
195
196：更新処理部
暗号処理部
140
記憶部
120
制御部
130
110：通信処理部
認証処理部
197
受信部
111
送信部
112
101
201
200：通信装置(被認証装置)
211
受信部
212
送信部
210：通信処理部
220
記憶部
230
制御部
297
認証処理部
乱数生成部
250
一時鍵生成部
280
暗号処理部
240
更新用データチェック部
290
更新確認データ生成部
295
296：更新処理部

図2

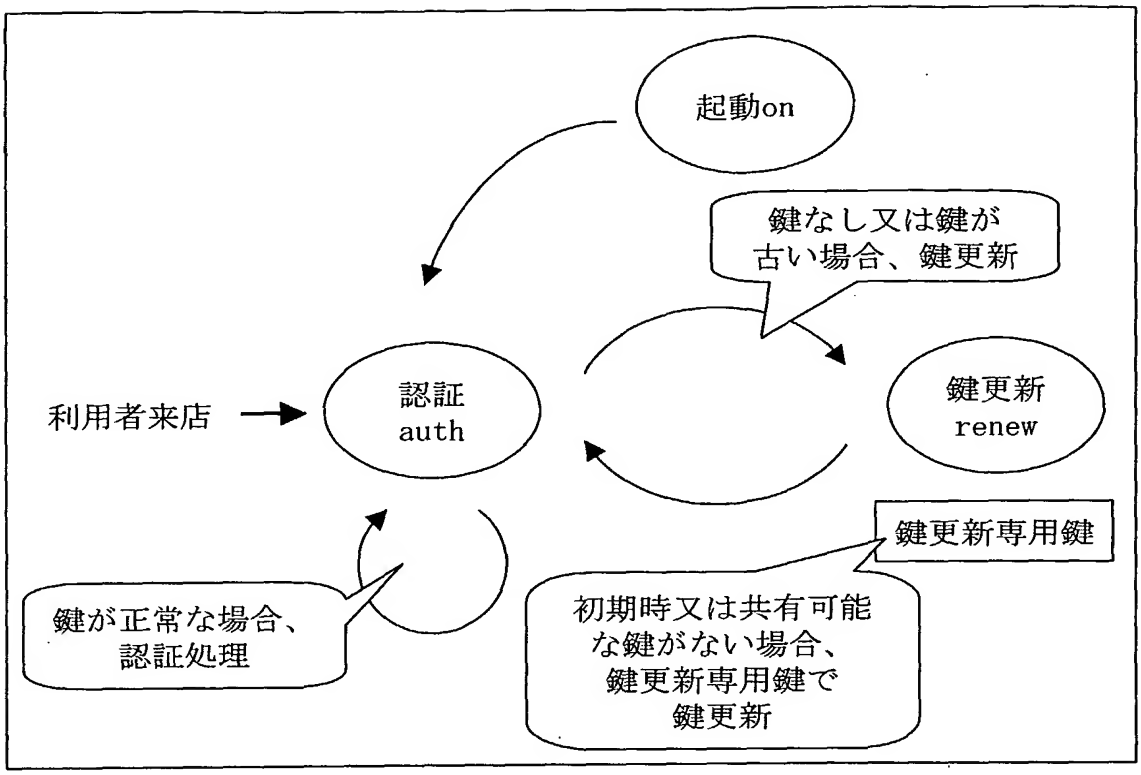

起動on
鍵なし又は鍵が
古い場合、鍵更新
利用者来店
認証
auth
鍵更新
renew
鍵更新専用鍵
鍵が正常な場合、
認証処理
初期時又は共有可能
な鍵がない場合、
鍵更新専用鍵で
鍵更新

図3

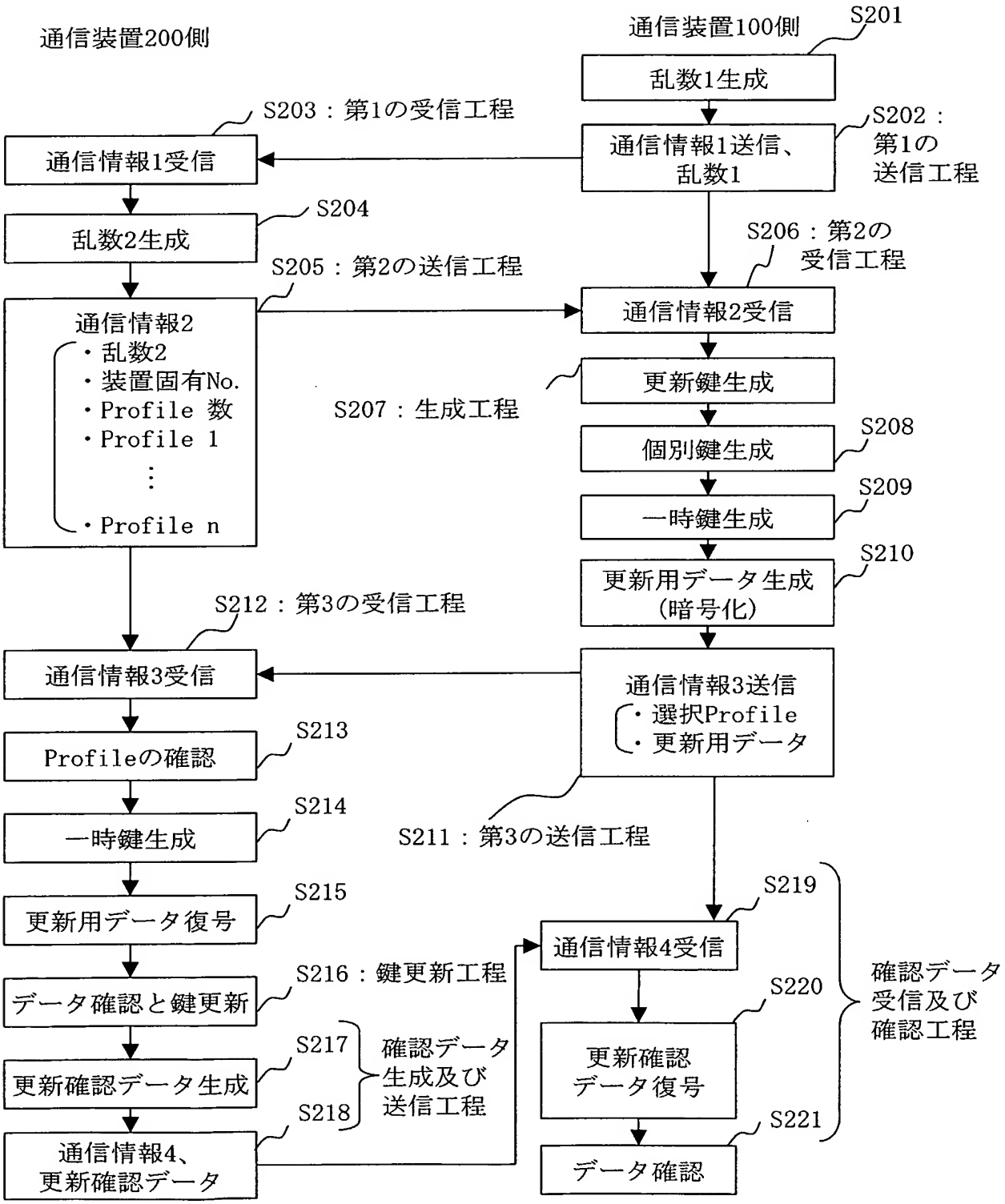

通信装置200側
通信装置100側
S201
乱数1生成
S203：第1の受信工程
通信情報1受信
通信情報1送信、
乱数1
S202：
第1の
送信工程
S204
乱数2生成
S206：第2の
受信工程
S205：第2の送信工程
通信情報2
・乱数2
・装置固有No.
・Profile 数
・Profile 1
・Profile n
通信情報2受信
更新鍵生成
S207：生成工程
S208
個別鍵生成
S209
一時鍵生成
S210
更新用データ生成
(暗号化)
S212：第3の受信工程
通信情報3受信
通信情報3送信
・選択Profile
・更新用データ
S213
Profileの確認
S214
一時鍵生成
S211：第3の送信工程
S215
更新用データ復号
S219
通信情報4受信
S216：鍵更新工程
データ確認と鍵更新
S220
更新確認
データ復号
確認データ
受信及び
確認工程
S217
更新確認データ生成
確認データ
生成及び
送信工程
S218
通信情報4、
更新確認データ
S221
データ確認

図4

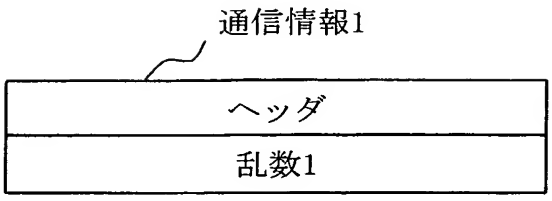

通信情報1
ヘッダ
乱数1

図5

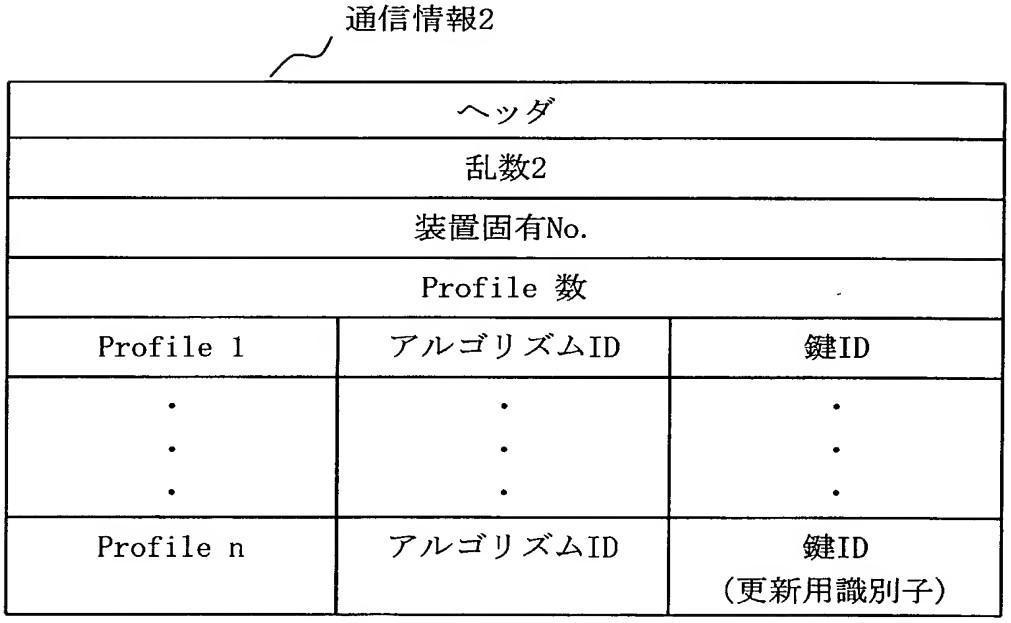

通信情報2
ヘッダ
乱数2
装置固有No.
Profile 数
Profile 1
アルゴリズムID
鍵ID
Profile n
アルゴリズムID
鍵ID
(更新用識別子)

図6

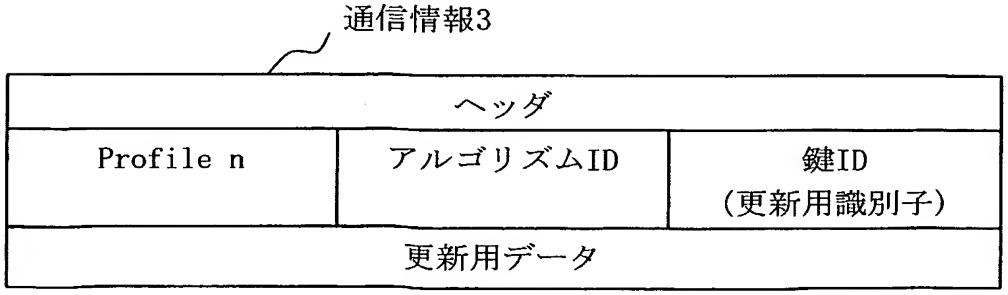

通信情報3
ヘッダ
Profile n
アルゴリズムID
鍵ID
(更新用識別子)
更新用データ

図7

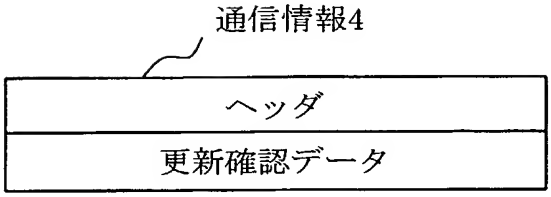

通信情報4
ヘッダ
更新確認データ

図8

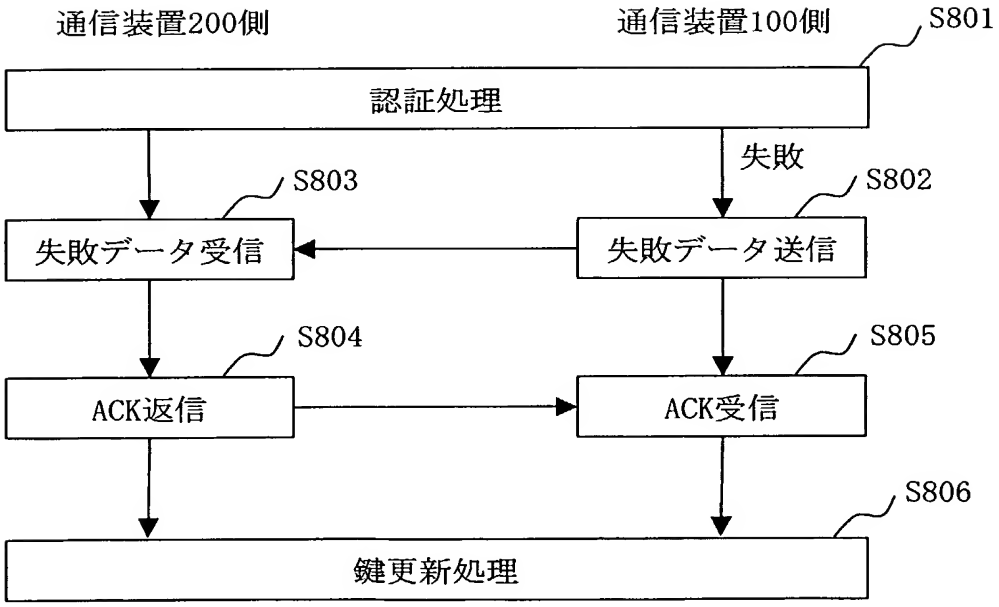
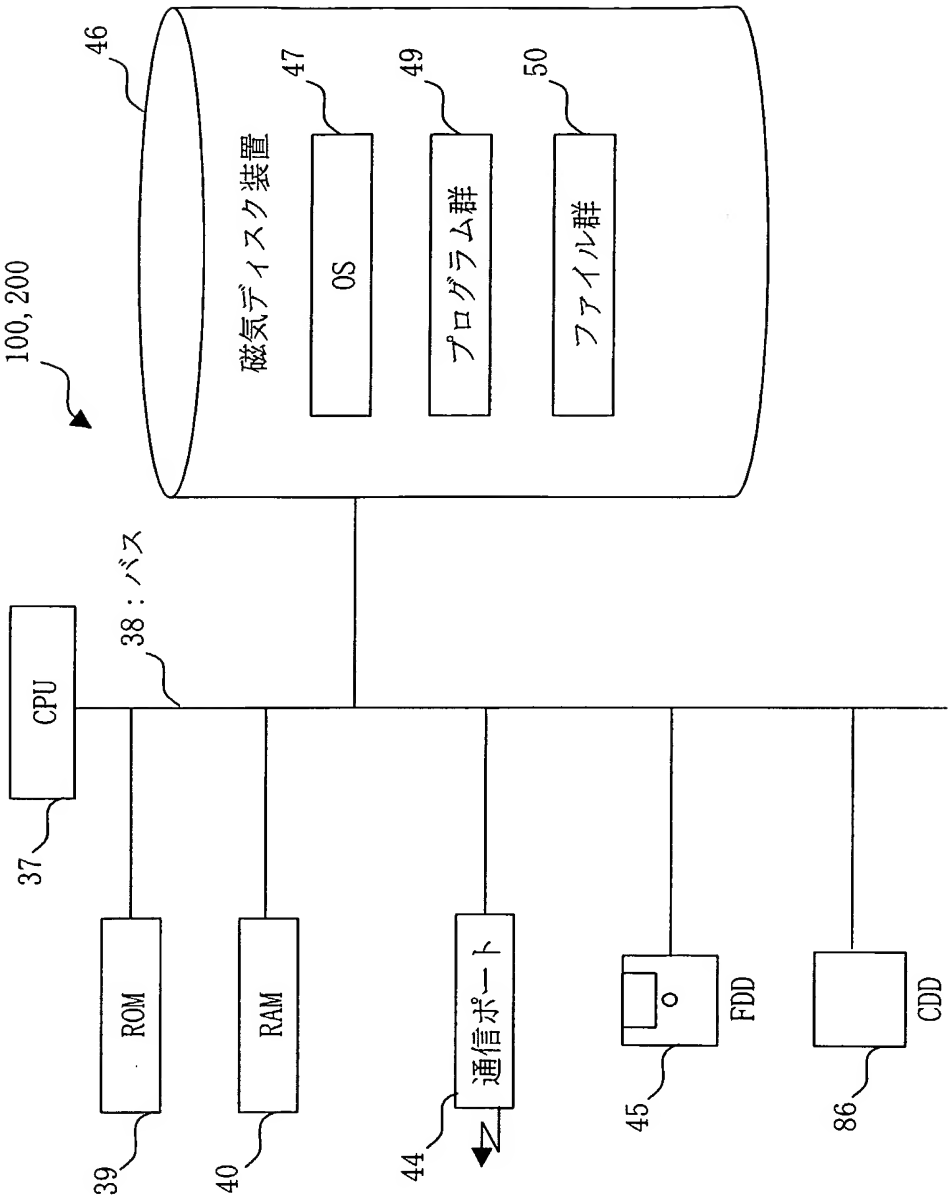

通信装置200側
通信装置100側
S801
認証処理
失敗
S803
S802
失敗データ受信
失敗データ送信
S804
S805
ACK返信
ACK受信
S806
鍵更新処理

図9


46
磁気ディスク装置
47
OS
49
プログラム群
50
ファイル群
100, 200
38：バス
CPU
37
ROM
39
RAM
40
通信ポート
44
FDD
45
CDD
86

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/005879

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, H04L9/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, H04L9/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-357370 A (Sony Corp.), 26 December, 2001 (26.12.01), Figs. 41 to 50 (Family: none)	1-6
A	JP 11-85014 A (Teruo MATSUMOTO), 30 March, 1999 (30.03.99), Par. No. [0017] (Family: none)	1-6

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 14 July, 2004 (14.07.04)	Date of mailing of the international search report 03 August, 2004 (03.08.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００５８７９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ　９／３２，Ｈ０４Ｌ　９／１４

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ　９／３２，Ｈ０４Ｌ　９／１４

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　　１９２２－１９９６年
日本国公開実用新案公報　１９７１－２００４年
日本国登録実用新案公報　１９９４－２００４年
日本国実用新案登録公報　１９９６－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００１－３５７３７０　Ａ（ソニー株式会社） ２００１．１２．２６，第４１－５０図　（ファミリーなし）	１－６
Ａ	ＪＰ　１１－８５０１４　Ａ（松本輝夫） １９９９．０３．３０，【００１７】段落　（ファミリーなし）	１－６

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１４．０７．２００４	03.8.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	石田　信行	５Ｍ　９４６９
	電話番号　０３－３５８１－１１０１　内線　３５９８	